The George Washington Law Review Presents

Hacking into the Computer Fraud and Abuse Act: The CFAA at 30

November 6, 2015

Symposium Schedule*

8:30 – 9:15 AM: Registration and Breakfast

- **Location**: Kelly Lounge, The GW Law School

9:15 – 10:00 AM: Opening Remarks

- **Location**: Moot Court Room, The GW Law School
- **Introduction and Welcome**: Bradford R. Clark, William Cranch Research Professor of Law, The George Washington Law School
- **Keynote Address**: David Bitkower, Principle Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice

10:00 – 10:50 AM: PANEL 1: What is Unauthorized Access? Part 1

- **Location**: Moot Court Room, The GW Law School
- **Panelists**: Matthew Kugler, Law Clerk, The Honorable Richard Posner
  - *Measuring Computer Use Norms*
- Josh Goldfoot
  - *A Trespass Framework for the Crime of Hacking* (with Aditya Bamzai)
- Aditya Bamzai
  - *A Trespass Framework for the Crime of Hacking* (with Josh Goldfoot)

10:50 – 11:05 AM: Coffee Break and Panel Transition

- **Location**: Kelly Lounge, The GW Law School

***PLEASE SEE THE MAP IN THE BACK OF THIS BROCHURE FOR LOCATIONS**

Symposium Schedule (Continued)

11:05 AM – 12:20 PM: PANEL 2: What is Unauthorized Access? Part 2

- **Location**: Moot Court Room, The GW Law School
- **Panelists**: Patricia L. Bellia, Professor of Law, Notre Dame Law School
  - *A Code-Based Approach to Unauthorized Access*
- Michael J. Madison, Professor of Law, Pitt Law
  - *Authority and Authorship*
- James Grimmelmann, Professor of Law, Maryland Law
  - *Consenting to Computer Use*

12:20 – 2:00 PM: Lunch

- **Location**: Law Learning Center Lobby, The GW Law School

2:00 – 2:50 PM: PANEL 3: The Debate over *United States v. Nosal*

- **Location**: Moot Court Room, The GW Law School
- **Panelists**: William A. Hall
  - *The Ninth Circuit's Deficient Examination of the Legislative History of the "Exceeds Authorized Access" Provision of the Computer Fraud and Abuse Act in* United States v. Nosal
- Jonathan Mayer, Junior Affiliate Scholar, Center for Internet and Society, Stanford Law School
  - *What Did* Nosal *Do?: Understanding the "Narrow" Interpretation of the Computer Fraud and Abuse Act*

2:50 – 3:05 PM: Coffee Break and Panel Transition

- **Location**: Kelly Lounge, The GW Law School

3:05 – 4:45 PM: PANEL 4: Beyond Authorization: Proposed Changes to the CFAA

- **Location**: Moot Court Room, The GW Law School
- **Panelists**: Orin Kerr, Fred C. Stevenson Research Professor of Law, The GW Law School
  - *Trespass, Not Theft: Rethinking Sentencing Under the Computer Fraud and Abuse Act*
- Ric Simmons, Chief Justice Thomas J. Moyer Professor for the Administration of Justice and Rule of Law, Ohio State Law School
  - *The Impossible Task of the Computer Fraud and Abuse Act: Time to Take a New Approach to Regulating Computer Crime*
- Michael Levy, Chief, Computer Crimes Section, U.S. Attorney's Office for the Eastern District of Pennsylvania
  - *A Proposed Amendment to 18 U.S.C. § 1030 – The Problem of Employee Theft*
- Paul Ohm, Professor of Law, Georgetown Law
  - *The Children of the CFAA: The Expanding Regulation of Code under Federal Law* (writing with Blake E. Reid)

4:45 – 6:45 PM: Reception

- **Location**: Tasher Great Room, The GW Law School

Opening Remarks

Keynote address: David Bitkower, Principal Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice

David Bitkower is the Principal Deputy Assistant Attorney General for the Criminal Division of the Department of Justice, and assists the Assistant Attorney General in the supervision of the Division's more than 600 federal prosecutors who conduct investigations and prosecutions involving fraud, public corruption, cybercrime, intellectual property, organized and transnational crime, money laundering, child exploitation, and other matters. Prior to his appointment as Principal Deputy Assistant Attorney General, Mr. Bitkower served as a Deputy Assistant Attorney General, and supervised the Criminal Division's Computer Crime and Intellectual Property Section, Organized Crime and Gang Section, and Human Rights and Special Prosecutions Section. Before joining the Criminal Division, Mr. Bitkower served as an Assistant United States Attorney for the Eastern District of New York, most recently as Chief of the National Security and Cybercrime Section. In that role, he oversaw counterterrorism, counterespionage, international organized crime and cybercrime prosecutions, among others. Mr. Bitkower has also personally prosecuted some of the country's most significant and high- profile terrorism cases, including serving as the lead prosecutor in the cases involving the 2009 Al-Qaeda plot to attack the New York City subway system. Mr. Bitkower was also previously detailed to work at the Department of Justice's National Security Division and on the President's Guantanamo Bay Review Task Force. Before joining the Department, Mr. Bitkower was a law clerk to U.S. Circuit Judge Pierre N. Leval of the Second Circuit Court of Appeals and to U.S. District Judge Leonard B. Sand of the Southern District of New York. Mr. Bitkower is a graduate of Yale University and earned his law degree from Harvard Law School.

Introduction by: Bradford R. Clark, William Cranch Research Professor of Law, The George Washington Law School

Professor Clark teaches and writes in the areas of civil procedure, constitutional structure, federal courts, and foreign relations. His scholarship has appeared in leading journals including California Law Review, Columbia Law Review, Harvard Law Review, Texas Law Review, University of Chicago Law Review, University of Pennsylvania Law Review, and Virginia Law Review. Professor Clark has been a visiting professor at Harvard Law School and the University of Michigan Law School. Professor Clark also served as a special master appointed by the Supreme Court to make recommendations in an original action between states, Alabama, et al. v. North Carolina, Orig. No. 132.

Before joining the Law School faculty, Professor Clark spent several years practicing law in the Washington, D.C. office of Gibson, Dunn & Crutcher, where he specialized in trial and appellate litigation. Previously, he served as an attorney adviser in the Department of Justice's Office of Legal Counsel, where he provided legal advice to the president, the attorney general, and the heads of executive departments. Professor Clark also served as a law clerk to The Honorable Robert H. Bork of the U.S. Court of Appeals for the D.C. Circuit and to The Honorable Antonin Scalia of the Supreme Court of the United States.

PANEL 1: What is Unauthorized Access? Part 1

- **Location**: Jacob Burns Moot Court Room, The GW Law School
- **Panelists**: Matthew Kugler, Law Clerk, The Honorable Richard Posner
- Josh Goldfoot
- Aditya Bamzai

Measuring Computer Use Norms

Matthew Kugler

The Computer Fraud and Abuse Act prohibits unauthorized use of computer systems. Courts have had trouble defining unauthorized use, however, with many potential answers risking overbreadth. One proposed solution is to use the norms of actual computer users to help define authorization, restricting punishment to that which many or all agree to be unauthorized. This study measures lay authorization beliefs and punishment preferences for a variety of computer misuse activities. Though perceived authorization was strongly predictive of punishment attitudes, results show that many people view common misuse activities as unauthorized but not deserving of any meaningful punishment. Respondents also viewed as unauthorized many activities – such as ignoring a website's terms of service, surfing the news while at work, or connecting to a neighbor's unsecured wireless network – that scholars have argued need are implicitly licensed. This divergence between perceived authorization and desired punishment presents a challenge for the CFAA framework. To avoid results that would strike both the lay public and field experts as overcriminalization, "unauthorized use" must therefore be interpreted far more narrowly than common usage would suggest.

Author Biography: Matthew Kugler graduated from the University of Chicago Law School in June, 2015. He is now a law clerk for the Honorable Richard A. Posner. Prior to law school, Matthew received his BA in psychology and political science from Williams College in 2005. He then completed a Ph.D. in Psychology and Social Policy at Princeton University under the supervision of Drs. Joel Cooper and John Darley in 2010 and was a postdoctoral fellow and adjunct instructor in psychology at Lehigh University in Bethlehem.

His research addresses questions at the intersection of psychology and law. He is particularly interested in issues of intellectual property, privacy, and criminal procedure.

A Trespass Framework for the Crime of Hacking

Josh Goldfoot† and Aditya Bamzai†

We argue that "authorization" in the CFAA should be interpreted consistent with the authorization rules governing physical trespass. The CFAA reflects Congress's judgment that computer owners who connect their computers to networks (like the Internet) have the right to regulate who may connect to their computer, and, once connected, what may be done with their computer. In short, Congress hoped to mimic trespass protections. Under common law, a trespass is "without authorization" if (a) it violates an express or implied prohibition on access; (b) the violator knew, or should have known, of the prohibition's existence; and (c) the prohibition on access advances the rationale for the crime of trespass. We apply the same rules to authorization under CFAA, and conclude the statute draws sensible, defensible distinctions and is not void for vagueness.

---

† Author is writing and presenting in his personal capacity. The ideas, views, and opinions expressed are his own and are not those of the United States Department of Justice.

Author Biography: Josh Goldfoot is Deputy Chief for Cyber Policy in the Department of Justice's National Security Division (but is participating in this symposium in his personal capacity). He has worked in the Department on computer security, computer crime, and online investigation issues for ten years. He has worked in technology law since 1999, when he advised Internet startups in Silicon Valley on intellectual property issues. Prior to joining the Department of Justice in 2005, he litigated civil cases, and clerked for judge Alex Kozinski on the Ninth Circuit U.S. Court of Appeals. He has authored or co-authored three law review articles about law and technology: The Physical Computer and the Fourth Amendment (2011); A Declaration of the Dependence of Cyberspace (2009), and Antitrust Implications of Internet Administration (1998). He received a United States patent in 2008 for shape recognition technology.

Author Biography: Aditya Bamzai is an attorney on the appellate staff of the National Security Division at the United States Department of Justice (but is participating in this symposium in his personal capacity). He is a former law clerk to Justice Antonin Scalia of the United States Supreme Court and Judge Jeffrey Sutton of the Sixth Circuit Court of Appeals, and a graduate of the University of Chicago Law School and Yale University.

PANEL 2: What is Unauthorized Access? Part 2

- **Location**: Jacob Burns Moot Court Room, The GW Law School
- **Panelists**: Patricia L. Bellia, Professor of Law, Notre Dame Law School
- Michael J. Madison, Professor of Law, Pitt Law
- James Grimmelmann, Professor of Law, Maryland Law

A Code-Based Approach to Unauthorized Access

Patricia L. Bellia

The Computer Fraud and Abuse Act imposes civil and criminal liability for "access" to a protected computer that is "without authorization" or that "exceed[s] authorized access." Plaintiffs seeking to control access to their network resources – including both closed and open systems – have pressed courts to apply the concept of unauthorized access to a range of behavior, including breach of the terms dictating use of the system, breach of other contractual provisions, behavior inconsistent with the system owner's reasonable expectations, and so forth. Courts are deeply divided on these claims, and that division has carried over to interpretations of state analogues to the CFAA, as well as to another federal statute that targets unauthorized access, the Electronic Communications Privacy Act. In this Essay, I defend a "code-based" approach to unauthorized access to systems under the Computer Fraud and Abuse Act and related statutes. Such an approach is faithful to the text and history of the CFAA, and best balances the relevant normative considerations.

Author Biography: Patricia L. Bellia teaches and researches in the areas of constitutional law, administrative law, cyberlaw, electronic surveillance law, and copyright law. She is co-author of a leading cyberlaw casebook and has published several articles on internet law (particularly surveillance and privacy issues) and separation of powers. Professor Bellia joined the Notre Dame faculty in 2000 and has also served as a visiting professor at the University of Virginia Law School (2007).

Professor Bellia earned her A.B. summa cum laude from Harvard University in 1991, where she was elected to Phi Beta Kappa. Before attending the Yale Law School, she worked at the Carnegie Endowment for International Peace, serving as an editor for Foreign Policy magazine and co-authoring a book on self-determination movements. At Yale, she served as editor-in-chief of the Yale Law Journal, executive editor of the Yale Journal of International Law, and student director of the Immigration Legal Services clinic. Upon graduation in 1995, she clerked for Judge José A. Cabranes of the United States Court of Appeals for the Second Circuit and Associate Justice Sandra Day O'Connor of the Supreme Court of the United States. Following her clerkships, Professor Bellia worked for three years as an attorney-advisor in the Office of Legal Counsel of the United States Department of Justice.

Since 2009, Professor Bellia has served as the chair of the University's Faculty Board on Athletics (FBA), the principal advisory group to the President on educational issues related to intercollegiate athletics. The committee monitors data on the admission of student-athletes and their academic performance, progress toward degrees, and graduation rates. It also assesses the effectiveness of institutional support for student-athletes. In addition to chairing the FBA, Professor Bellia serves as Notre Dame's faculty athletics representative to the National Collegiate Athletic Association.

Authority and Authorship

Michael J. Madison

As a copyright scholar, I notice an unmistakable conceptual as well as terminological affinity between the idea of "authorship" in intellectual property law, as a legal device meant to regulate access to intellectual works, and the idea of "authority" in information security law, as a legal device meant to regulate access to computer networks.

This short paper highlights for security law purposes a lesson that is increasingly clear in copyright contexts: that both authority and authorship are not only contextual, but also are products of audience or user construction rather than matters of creator or designer intent. In that regard, this paper revives and refines a proposal that I made a dozen years ago (44 B.C.L. Rev. 433 (2003)), to the effect that authority and access in the context of the CFAA are best viewed as matters of shared or collective user experience, rather than as matters of technological design as such or as matters of subjective user intent.

Author Biography: Professor Michael Madison is Professor of Law and Faculty Director of the Innovation Practice Institute at the University of Pittsburgh School of Law. He writes and teaches about intellectual property law and policy, and about questions concerning the production and distribution of knowledge and innovation. He is the author of more than 30 journal articles and book chapters, the co-author of The Law of Intellectual Property (Wolters Kluwer, 4th edition 2013) and the co-editor of Governing Knowledge Commons (Oxford University Press 2014).

Professor Madison is the co-founder of the global research network titled the Workshop on Governing Knowledge Commons. Classroom subjects include various disciplines of intellectual property law, contracts and commercial law, and property law. His research and scholarship address the emerging discipline of knowledge commons, governance of innovation institutions, and knowledge as a subject of legal regulation. He joined the Pitt Law faculty in 1998. Before becoming a law professor, Professor Madison practiced law in San Francisco and Silicon Valley for nine years. He received his JD from Stanford University and his BA from Yale.

Consenting to Computer Use

James Grimmelmann

"Authorization" under the CFAA is a confusing question for the same reason consent is a confusing question throughout the law: the concept itself is ambiguous. Drawing on a taxonomy of consent developed by Peter Westen, I will argue that we can better understand controversies about the proper scope of the CFAA if we distinguish between the factual question of what uses a computer owner actually expressed consent to, and the legal question of when a user will be treated as having acted with the owner's consent. Factual consent is the baseline from which legal consent starts, but it is neither necessary nor sufficient. Sometimes, a computer owner's factual consent is ineffective due to fraud; sometimes, the legal system imputes consent she did not actually give. These decisions are irreducibly normative, and they cannot be made simply by looking to the text of the CFAA.

Author Biography: James Grimmelmann is a Professor of Law at the University of Maryland Francis King Carey School of Law and a Visiting Professor at the University of Maryland Institute for Advanced Computer Studies. He previously taught at New York Law School and the Georgetown University Law Center. He holds a J.D. from Yale Law School and an A.B. in computer science from Harvard College. Prior to law school, he worked as a programmer for Microsoft. He has served as a Resident Fellow of the Information Society Project at Yale, and as a law clerk to the Honorable Maryanne Trump Barry of the United States Court of Appeals for the Third Circuit.

He studies how laws regulating software affect freedom, wealth, and power. As a lawyer and technologist, he helps these two groups understand each other by writing about copyright, search engines, privacy, and other topics in computer and Internet law. He is the author of the casebook Internet Law: Cases and Problems, now in its fifth edition. He has been blogging since 2000 at the Laboratorium (http://laboratorium.net/), and his home page is at http://james.grimmelmann.net/.

PANEL 3: The Debate over *United States v. Nosal*

- **Location**: Jacob Burns Moot Court Room, The GW Law School
- **Panelists**: William A. Hall
- Jonathan Mayer, Junior Affiliate Scholar, Center for Internet and Society, Stanford Law School

The Ninth Circuit's Deficient Examination of the Legislative History of the "Exceeds Authorized Access" Provision of the Computer Fraud and Abuse Act in *United States v. Nosal*

William Hall†

In *United States v. Nosal*, the en banc Ninth Circuit significantly limited the scope of our country's main computer crime statute, the Computer Fraud and Abuse Act ("CFAA"). *Nosal* marked the first instance where a federal circuit court has held that that the government may not prosecute so-called "insider" cases under the CFAA where information was knowingly obtained or altered for a purpose prohibited by the computer owner. In doing so, the Ninth Circuit claimed that its interpretation of the CFAA was "a more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking – the circumvention of technological access barriers – not misappropriation of trade secrets – a subject Congress has dealt with elsewhere." This article will examine the *Nosal* en banc opinion, focusing on its claims concerning the legislative history of the CFAA, and then will explore the legislative history of the CFAA and its subsequent amendments. This review will demonstrate that, contrary to the Ninth Circuit's reading of the CFAA, Congress's clear intent was to permit prosecutions of insiders who access information on a computer system for a purpose prohibited by the owner of the system.

Author Biography: William ("Bill") A. Hall, Jr. is a Senior Trial Attorney in the Computer Crime and Intellectual Property Section ("CCIPS") of the U.S. Department of Justice ("DOJ") in Washington, D.C., where he specializes in the investigation and prosecution of computer crime cases, particularly those involving computer intrusions, fraud, and threats to national security. Prior to joining CCIPS, Bill served as Counsel on the Judiciary Committee of the U.S. Senate, where he specialized in crime and terrorism issues; as an Assistant U.S. Attorney in San Diego, California, where he handled computer, white collar, and child exploitation cases; as a Trial Attorney in the Child Exploitation and Obscenity Section of DOJ; and, as an Assistant District Attorney in Philadelphia, Pennsylvania. He also clerked for Judge Danny Boggs of the U.S. Court of Appeals for the Sixth Circuit. He is a graduate of Dartmouth College and Harvard Law School.

---

† Author is writing and presenting in his personal capacity. The ideas, views, and opinions expressed are his own and are not those of the United States Department of Justice.

What Did *Nosal* Do?: Understanding the "Narrow" Interpretation of the Computer Fraud and Abuse Act

Jonathan Mayer

In the seminal *United States v. Nosal* opinion, a panel of the Ninth Circuit broke with every prior appellate ruling and sharply narrowed liability under the Computer Fraud and Abuse Act (CFAA). Lower courts have overwhelmingly followed *Nosal*, as has the Fourth Circuit. The state of doctrine after *Nosal*, though, remains a subject of widespread confusion among practitioners and scholars.

This article attempts to clarify what *Nosal* held, and how lower courts have developed its "narrow" interpretation of CFAA into a surprisingly coherent body of law. The *Nosal* doctrine, I explain, is distinct from prior readings of CFAA that borrow from agency principles, contract law, or technical access controls. Rather, *Nosal* reflects a novel middle ground, moderating CFAA's scope while maintaining a firm foundation in legislative text and history.

Author Biography: Jonathan Mayer is a Ph.D. candidate in computer science and a lawyer at Stanford University, where he received his J.D. in 2013. He was named one of the Forbes 30 Under 30 in 2014, for his work on technology security and privacy. Jonathan's research and commentary frequently appear in national publications, and he has contributed to federal and state law enforcement actions.

Jonathan is a Cybersecurity Fellow at the Center for International Security and Cooperation, a Junior Affiliate Scholar at the Center for Internet and Society, and a Stanford Interdisciplinary Graduate Fellow. He earned his A.B. at Princeton University in 2009, concentrating in the Woodrow Wilson School of Public and International Affairs.

PANEL 4: Beyond Authorization: Proposed Changes to the CFAA

- **Location**: Jacob Burns Moot Court Room, The GW Law School
- **Panelists:** Orin Kerr, Fred C. Stevenson Research Professor of Law, The GW Law School
- Ric Simmons, Chief Justice Thomas J. Moyer Professor for the Administration of Justice and Rule of Law, Ohio State Law School
- Michael Levy, Chief, Computer Crimes Section, U.S. Attorney's Office for the Eastern District of Pennsylvania
- Paul Ohm, Professor of Law, Georgetown Law

Trespass, Not Theft: Rethinking Sentencing Under the Computer Fraud and Abuse Act
Orin Kerr

This article argues that the sentencing regime for CFAA crimes uses the wrong set of principles. Since 1988, the Federal Sentencing Guidelines have treated CFAA crimes as a subset of theft offenses. They have used the loss chart for theft crimes by which the more a person steals the greater the punishment should be. This basic framework is wrong. CFAA offenses are trespass crimes, not theft crimes. Losses are consequential harms, not wrongful gains by the defendant. As a result, CFAA crimes should be sentenced under a new Guideline just for CFAA offenses rather than squeezed into the poor fit of the existing economic crimes guideline. The new CFAA guideline should consider consequential losses, but not as the primary way to determine the seriousness of the crime.

Author Biography: Professor Kerr is a nationally recognized scholar of criminal procedure and computer crime law. He has authored more than 50 articles, and his scholarship has been cited in over 150 judicial opinions and more than 2000 academic works. Before joining the faculty in 2001, Professor Kerr was a trial attorney in the Computer Crime and Intellectual Property Section at the U.S. Department of Justice, as well as a Special Assistant U.S. Attorney in the Eastern District of Virginia. He is a former law clerk for Justice Anthony M. Kennedy of the U.S. Supreme Court and Judge Leonard I. Garth of the U.S. Court of Appeals for the Third Circuit. Professor Kerr has argued cases in the United States Supreme Court and the Third, Fourth, and Sixth Circuits. He has testified six times before Congressional committees. In 2013, Chief Justice Roberts appointed Professor Kerr to serve on the Advisory Committee for the Federal Rules of Criminal Procedure.

Professor Kerr has been a visiting professor at the University of Chicago and the University of Pennsylvania, and he served as a scholar-in-residence at the Law Library of Congress from 2012 to 2014. In the summer of 2009 and 2010, he served as special counsel for Supreme Court nominations to Senator John Cornyn on the Senate Judiciary Committee. The GW Law Class of 2009 awarded Professor Kerr the Law School's teaching award. He posts regularly at the popular blog The Volokh Conspiracy. Before attending law school, he earned undergraduate and graduate degrees in mechanical engineering.

The Impossible Task of the Computer Fraud and Abuse Act: Time to Take a New Approach to Regulating Computer Crime

Ric Simmons

This article uses the Computer Fraud and Abuse Act ("CFAA") as a case study to examine the challenges posed by regulating criminal activity with respect to a specific and evolving technology. The original provisions of the CFAA were written to apply to computers that are now almost unrecognizable and which were created at a time when computers played a markedly different role in society. This article examines how computers and society's norms in relationship to computers have evolved over the past thirty years, and how the CFAA has been unable to keep pace with these changes. The article proposes that the best way to regulate and criminalize misconduct involving computers--as with any rapidly evolving technology--is by allowing pre-existing criminal statutes to cover the more traditional manifestations of computer crime (those involving fraud, theft, and criminal damaging) and creating an administrative agency to regulate the only truly "unique" computer crime: unauthorized access. The problem of unauthorized access has posed the most challenges with regard to the CFAA over the past thirty years, and shifting the burden of enforcing this aspect of computer crime to an administrative agency solves many of those problems.

Author Biography: Professor Ric Simmons is the Chief Justice Thomas J. Moyer Professor for the Administration of Justice and Rule of Law at Moritz College of law at The Ohio State University. He is a graduate of Columbia Law School, where he was a Stone Scholar and a senior editor of the Columbia Law Review. Following law school, he clerked for the Honorable Laughlin E. Waters of the Central District of California and then served for four years as an assistant district attorney for New York County. He was an acting assistant professor at New York University School of Law from June 2000 through June 2003 and before moving to Moritz.

Professor Simmons' research focuses on the intersection of the Fourth Amendment and new technology. He has written about searching cell phones, the use of new surveillance techniques, and hyper-intrusive surveillance. He has also written about the privatization of the criminal justice system. Professor Simmons has been frequently cited in the local and national media on criminal procedure issues.

Professor Simmons has also co-authored two casebooks: Learning Evidence: From the Federal Rules to the Courtroom (with co-author Debby Merritt) (3rd ed. 2014 West Publishing) and Learning Criminal Procedure (with co-author Renee Hutchins) (2014 West Publishing). He teaches Evidence, Criminal Law, Criminal Procedure, and Computer Crime and Surveillance.

A Proposed Amendment to 18 U.S.C. § 1030 – The Problem of Employee Theft

Michael L. Levy[†]

The problem of "unauthorized access" and the disloyal employee is one that plagues businesses in this country. Current interpretations of 18 U.S.C. § 1030(a)(2) are split on whether the statute covers the theft of data by an employee on his or her way out the door to a new job. Although there have been proposals to amend § 1030 to cover some of these scenarios, most of them are either inadequate or confusing. My proposal is to abandon efforts to deal with the authorization question and to focus on what concerns the victim – employees accessing the computers with the intent to steal information. My proposal is a statute, which makes it a crime to access a protected computer with the intent to steal information.

† Author is writing and presenting in his personal capacity. The ideas, views, and opinions expressed are his own and are not those of the United States Department of Justice.

Author Biography: Michael Levy is the Chief of Computer Crimes for the United States Attorney's office in the Eastern District of Pennsylvania. He has held that position since September 2001. From April 2001 to September 2001 and from May 2009 until May 2010, he served as the interim United States Attorney for the Eastern District of Pennsylvania until the confirmation of the presidential appointee. He has served in the U.S. Department of Justice since 1980 with two one-year excursions into private practice. He has prosecuted fraud, drug, tax, and organized crime cases, as well as handling civil and criminal forfeiture actions. From 1991 to 1993, he was the Deputy Chief of the Criminal Division. From 1993 until 2001, he was the First Assistant United States Attorney. As Chief of Computer Crime, Mr. Levy has prosecuted crimes involving intellectual property, computer intrusion, computer fraud, as well as federal crimes involving the sexual exploitation of children. Before joining the U.S. Attorney's office, Mr. Levy worked as a Public Defender (1970-73), as an Assistant District Attorney in Philadelphia (1973-74, 75-76), and as an Assistant Attorney General for the Commonwealth of Pennsylvania (1974-75). He also had his own law practice for four years. He is a 1966 graduate (cum laude) of Brown University and a 1969 Penn Law graduate. He teaches a seminar in Cybercrime at the University of Pennsylvania Law School.

The Children of the CFAA: The Expanding Regulation of Code under Federal Law
Paul Ohm & Blake E. Reid

Professor Ohm intends to compare our experience using the CFAA to constrain technologists with similar efforts, notably the DMCA's anti-circumvention provisions and the "willful or malicious interference" prohibition in the Telecommunications Act (47 U.S.C. 333). Professor Ohm hopes that this comparative effort will shed a little insight on proposals to reform the CFAA.

Author Biography: Paul Ohm is a Professor of Law at the Georgetown University Law Center. He specializes in information privacy, computer crime law, intellectual property, and criminal procedure. He teaches courses in all of these topics and more and he serves as a faculty director for the Center on Privacy and Technology at Georgetown. Before becoming a professor, he served as an Honors Program trial attorney in the U.S. Department of Justice's Computer Crime and Intellectual Property Section. In this capacity, he helped prosecute violations of the Computer Fraud and Abuse Act and helped develop DOJ policy regarding the law.

Author Biography: Blake E. Reid studies, teaches, and practices in the intersection of law, policy, and technology. He serves as the Director of the Samuelson-Glushko Technology Law & Policy Clinic (TLPC) and the Director of Fellowships and Special Projects at the Silicon Flatirons Center for Law, Technology, and Entrepreneurship. Before joining Colorado Law, he was a staff attorney and graduate fellow in First Amendment and media law at the Institute for Public Representation at Georgetown Law and a law clerk for Justice Nancy E. Rice on the Colorado Supreme Court.

Professor Reid is not presenting at the Symposium.

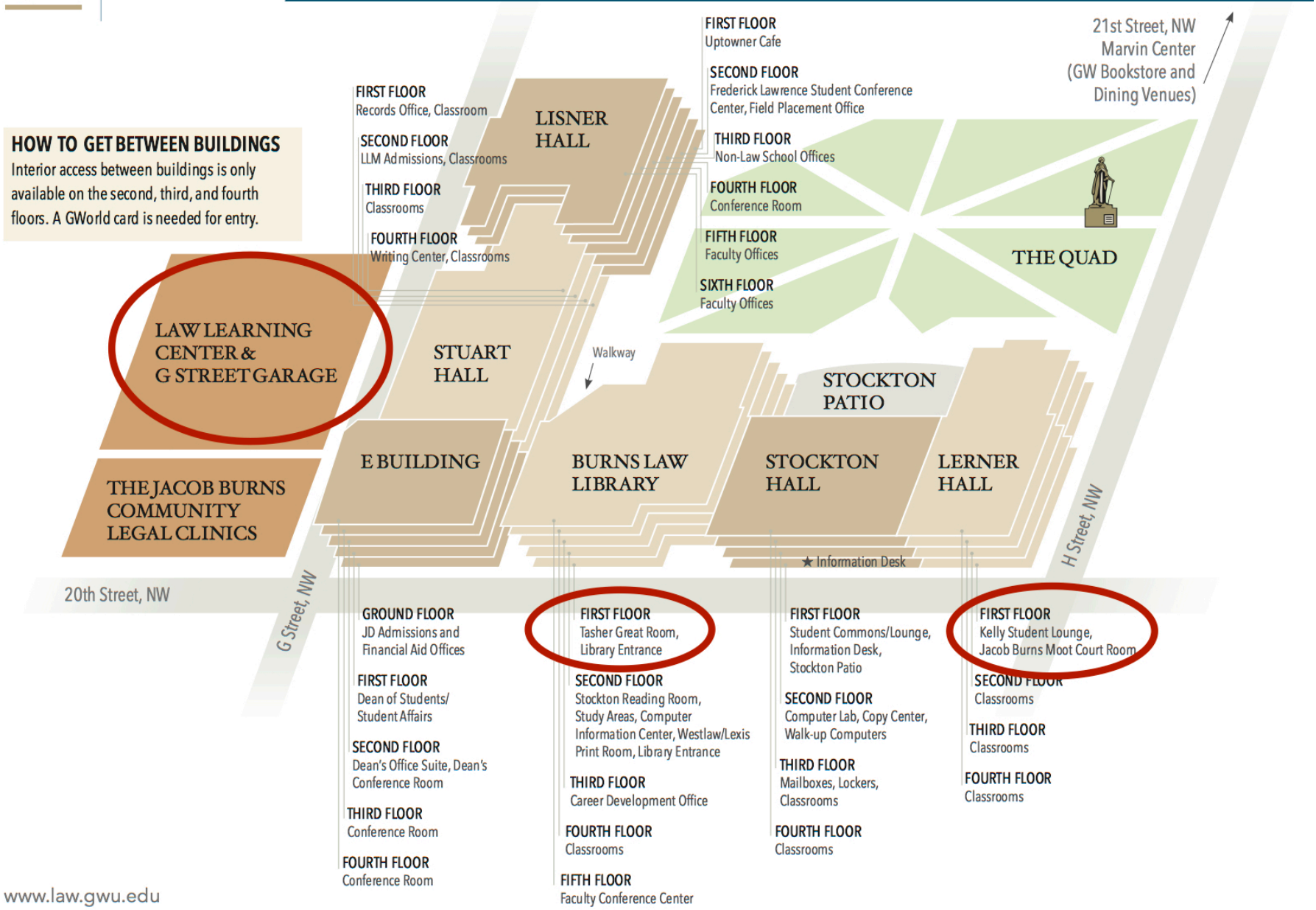
Thank you to all the panelists for their impressive contributions to this important subject. A special thank you to Professor Orin Kerr for co-hosting this Symposium with *The George Washington Law Review*. This event could not have occurred without the hard work of Carolyn Harris, Michelle Seares, Vladimir Semendyai, Alexandra Saper, and the rest of the *Law Review* staff. Find the complete articles in *The George Washington Law Review*'s special symposium issue, Volume 84, Issue 6 (forthcoming, 2016). More information about the *Law Review* is available on our website (http://www.gwlr.org/), Facebook (https://www.facebook.com/gwlawrevue), and Twitter (@GWLawReview).

GW | LAW

THE GEORGE WASHINGTON UNIVERSITY LAW SCHOOL • LAW SCHOOL COMPLEX

HOW TO GET BETWEEN BUILDINGS

Interior access between buildings is only available on the second, third, and fourth floors. A GWorld card is needed for entry.



www.law.gwu.edu

LAW_1314_1